nals (or clients) being observed during the communication session, even at a central communication hub (e.g., a teleconference mixer). The client terminals or the users of the client terminals may share secret keys with a trusted third party at a time that is convenient for secure communication, such as with a public key scheme with authentication, rather than when a communication session is about to commence.

In some embodiments, the trusted third party generates its own secret key and key switch hints from its private key and the client terminals' secret keys. The key switch hints are used to delegate decryption capability from the client to the third party and back again. After delegating decryption capability to a common key, resulting ciphertexts can be added together.

Embodiments of the invention may use a suitable encryption technique agreed-upon by each of the client terminals, for example, additive homomorphic encryption, such that all clients have a common private key. Client terminals may encode analog data signals (e.g., a user's voice) into a digital data stream using an additive encoding scheme, and encrypt the encoded digital data stream using a suitable encryption scheme, such as an additive homomorphic encryption scheme. The client terminals may then transmit the encrypted data stream to a central communication hub (e.g., a mixer), where the central communication hub operates to switch the encrypted data stream received from each client terminal into a representation that can be decrypted using the trusted third party private key. The central communication hub may then combine the switched data streams, for example, using an encrypted homomorphic addition. The central communication hub may then switch the combined switched data streams into a form that can be decrypted by an intended receiver using an appropriate key switch hint, and then send the result to the intended recipient. The recipient can then decrypt, decode, and play back the result.

FIG. **1** illustrates a distributed communication system **100** and plurality of entities or clients **102***a*-**102***d* engaging in electronic communication in a distributed communication system. The number of clients may vary according to the design and function of the communication system **100**. Each of the clients **102***a*-**102***d* includes one or more communication devices **104***a*-**104***d*, respectively. The communication devices **104***a*-**104***d* may be any suitable communication device configured to receive and process data communication signals over the distributed communication system **100**. In one embodiment, the communication devices **104***a*-**104***d* include Voice over Internet Protocol (VoIP) enabled telephones, capable of placing and transmitting telephone calls over an IP network (e.g., the Internet).

One or more of the communication devices **104***a*-**104***d* may also include a cellular telephone, smartphone, tablet computer, personal computer, or other suitable communication device with computing and connectivity capability that is capable of processing digital communications data, and transmitting and receiving digital communications data over a network. In one embodiment, one or more of the communication devices **104***a*-**104***d* may include a public switched telephone network (PSTN) telephone in electrical communication with an analog telephone adapter capable of converting analog data signals to digital data signals for communication over a digital communication network (e.g., the Internet). In the case of a PSTN telephone communication network, the distributed communication system may further include components capable of encoding, encrypting, and decrypting a digital communication signal for interface with the analog PSTN network. Each of the communication devices **104***a*-**104***d* may additionally include a microphone and a speaker for receiving and producing audible analog sound for users of the clients **102***a*-**102***d*.

Each of the client terminals **102***a*-**102***d* is in electronic communication with a central hub or mixer **106** by way of communication channels **108***a*-**108***d*, respectively. The central communication hub **106**, for example, a mixer, may be any suitable electronic mixer capable of combining two or more electrical or data signals into one or more composite output signals. In one embodiment, the mixer **106** is a VoIP-enabled mixer. The communication channels **108***a*-**108***d* may be uni-directional or bi-directional and transmit data between the clients **102***a*-**102***d* and the mixer **106** in a wired or wireless configuration.

During a communication session over the distributed communication network **100**, each of the clients **102***a*-**102***d* receive analog or digital data signals (e.g., audio and video provided by the user of the clients **102***a*-**102***d*), and provide a digital encrypted version of the analog or digital data signals over the respective communication channels **108***a*-**108***d* in the form of encrypted data streams **110***a*-**110***d*. For example, during a VoIP teleconference session, each of the clients **102***a*-**102***d* may sample analog voice data using the audio capturing capabilities of the respective communication devices **104***a*-**104***d*, encode the analog samples into digital data packets at regular intervals, and encrypt each of the digital data packets to create the encrypted data streams **110***a*-**110***d*. The encoded data packets may be encrypted into the encrypted data streams **110***a*-**110***d* using any suitable encryption scheme or algorithm, such as the NTRU encryption algorithm modified to provide either Somewhat Homomorphic Encryption (SHE) or Fully Homomorphic Encryption (FHE) capabilities.

The mixer **106** receives the encrypted data streams **110***a*-**110***d* from each of the clients **102***a*-**102***d*, respectively, and mixes the encrypted data streams **110***a*-**110***d* according to the design and function of the distributed communication network **100** to generate one or more composite encrypted result data steams **112***a*-**112***d*. The composite encrypted result data streams **112***a*-**112***d* may include a composite of all of the encrypted data streams **110***a*-**110***d*, or may selectively include only a portion of the encrypted data streams **110***a*-**110***d*. For example, the composite encrypted result data stream **112***a*, intended to be transmitted to the client **102***a*, may include a composite of all of the encrypted data streams **110***a*-**110***d*, or alternatively, may include only a composite of the encrypted data streams **110***b*-**110***d*, with the encrypted data stream **110***a* generated by the client terminal **102***a* not being included in the composite encrypted result data stream **112***a*, to improve the perceived sound quality for the user of the client terminal **102***a*.

After generating the composite encrypted result data streams **112***a*-**112***d*, the mixer **106** transmits the composite encrypted result data streams **112***a*-**112***d* to each of the client terminals **102***a*-**102***d*, respectively, by way of communication channels **114***a*-**114***d*. The communication channels **114***a*-**114***d* may be uni-directional or bi-directional and transmit data between the mixer **106** and the clients **102***a*-**102***d* in a wired or wireless configuration. Each of the clients **102***a*-**102***d* then decrypts the respective composite encrypted result data stream **112***a*-**112***d* that they receive using private or secret keys held by each of the clients **102***a*-**102***d*, and if necessary, decodes the decrypted data stream into an analog data stream, and plays the decoded and decrypted data stream using the corresponding communication device **104***a*-**104***d*.

According to the above process illustrated in FIG. **1**, each of the clients **102***a*-**102***d* transmits an encrypted data stream **110***a*-**110***d* to the central mixer **106** that is pre-encrypted.